Top Five Fraud Axioms IT Auditors Should Know

Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the ISACA Journal.

Somewhere in the career of the IT auditor, he/she will come across a piece of evidence of a fraud (and possibly not realize it is related to a fraud), discover a fraud or be asked to assist in a fraud investigation. Thus, one of the basic sets of knowledge the IT auditor needs is some essential information about fraud detection. This article attempts to identify some of the most important facts about fraud that are particularly applicable to the IT audit function. It is not intended to be an exhaustive list, but rather five things that would assist IT auditors in fulfilling their duties related to fraud in everyday tasks. These five are not ranked in any particular order.

1. PROFESSIONAL SKEPTICISM

One of the first things with which IT auditors need to get comfortable is the realistic view of the scope of fraud. According to the Association of Certified Fraud Examiners (ACFE), the total loss from fraud in any one year in the US is between 5 and 7 percent of gross revenues, with the latest statistic estimating total losses in the US economy at almost US $1 billion. One element of fraud that seems to occur frequently is the shock from the victim’s stakeholders that it happened to their entity. These facts are raison d’être for an antifraud program and/or fraud audit for any entity. So, the conclusion is twofold: Fraud has a vast scope, and it can happen anywhere. Therefore, it is important to be consistent with professional skepticism.

Also, the fraudster (white-collar criminal) is usually someone that is least suspected. In fact, fraudsters frequently do not look like crooks at all. Statistical profiles of white-collar criminals describe them as tending to be tenured at the entity, in a trusted position because they earned the trust of management, and relatively well educated. Again, professional skepticism is necessary to prevent one from being fooled, and, even then, there is a chance a fraudster can get away with a crime.

2. TOE IN THE WATER

One theory of fraud suggests that fraudsters begin their slippery slope into crime with a “test.” That is, they put together a fraudulent transaction or event and “float” it out into the entity’s environment to see if they can get away with the fraud. If that first instance gets noticed, the fraudster usually has a predetermined “excuse” for why it happened, often the “oops, I made a mistake” defense. If it goes unnoticed, the fraudster usually proceeds to the third item in this list.

The IT auditor needs to be aware that if he/she finds an unexplained anomaly or variance, and goes to the party responsible, and that person says “oops,” there is some probability, no matter how small, that it is a “test” transaction. The IT auditor should exercise due diligence in obtaining independent verification where feasible and should obtain it before approaching the party responsible for the transaction, where feasible—especially where circumstances increase suspicion. For example, in one fraud case, the auditor came to the responsible party and asked why a certain account amount was exactly double what it should have been. The accounting clerk stuttered, having been surprised, and the auditor himself gave the person an opportunity to use the “oops” defense, as he said to her, “You must have accidentally double paid the vendor.” In reality, it was a fraud scheme and not an overpayment.

3. ESCALATION OF THE CRIME

Most fraudsters who get caught tend to escalate their crime. This is substantiated by a variety of facts. ACFE’s regular Report to the Nation (RTTN), published in 1996, 2002, 2004, 2006 and 2008 (the 2010 version is currently being conducted), shows that, of the three main categories of fraud, there is an overlap in percentages because fraudsters were conducting frauds in more than one broad category. In one year, more than 4 percent of all frauds discovered and resolved included asset misappropriation, corruption and financial statement schemes by the fraudster.
Thus, the fraudster who floats the test and finds that it
goes unnoticed will decide to take more from the victim. That
can be done by committing more fraudulent transactions
in a shorter period of time, taking larger amounts in each
transaction or adding a new scheme. Again, this applies to
fraudsters who get caught, as no statistics exist for frauds
that go undiscovered. But, this escalation is good news to
those looking for evidence of fraud because it makes it easier
to discover. Therefore, the IT auditor should remember this
fact when performing data mining activities. For instance, a
trend analysis by a vendor that shows a significant increase
in purchases over time might be a red flag associated with an
escalation of a kickback scheme, shell vendor or other vendor-
related scheme. The same could be said about other analytical
procedures and accounts or classes of transactions.

For example, in one famous financial statement fraud, the
senior executives started out in 1986 with a simple scheme to
increase net income by about US $50,000. They worked hard
to fool the auditors and managed to do so for more than a
decade. By 2001, there were several schemes for that year,
and a batch of fictitious journal entries of more than
US $7 million alone.

4. TIP OF THE ICEBERG
Many times, a fraud is discovered by accident rather than as
a result of deliberate procedures. In such cases, usually an
astute auditor looked at a single event or transaction (e.g.,
a check for US $2,000), became suspicious for one reason
or another (often described by experts as “the smell test”),
and chose to dig deeper (e.g., to find dozens of other checks
totaling US $400,000 and another fraud scheme). This is the
“tip of the iceberg” theory. The first check was insignificant
in the amount, but if it is part of a sample, or one line of data
in an accounting file, it could be just one of many fraudulent
transactions. That is, when an anomaly comes to the attention
of the auditor, the auditor should stop and think about the
probability that this single anomaly is stand-alone or the
visible part of an “iceberg,” in which case the preponderance
of the mass is under water and out of sight. For instance, if
the IT auditor notices in the data that an employee received
two checks in one pay period for the same gross amount and
corporate policy does not allow for more than one check per
pay period, that circumstance would be an anomaly (a red
flag). Someone may provide a legitimate-sounding reason for
the duplication (“oops”), but the IT auditor should consider
drilling down on those facts to see if more fraud and/or
suspicious data exist.

This concept extends into the discovery of the fraudster. It
is fairly common for a fraudster who gets caught and chooses
to confess, to confess to the amount of fraud known up to that
point, or some amount that is far below the actual amount
(i.e., confesses to the tip of the iceberg or some amount
significantly less than the whole iceberg). Obviously, the
fraudster is hoping the victim will stop looking and deal with
the lesser amount. For example, the fraudster may decide it
is easier to confess to US $30,000 and pay it back, than to
admit to the actual US $400,000 fraud. Thus, the IT auditor
and fraud investigation team should consider a thorough fraud
audit to determine the amount of loss independent of the
fraudster, to the degree practicable. That subsequent fraud
audit is likely to benefit from data mining and data analysis by
the IT auditor.

5. DATA MINING AND ANALYSIS
Generally speaking, data can be invaluable in a fraud
investigation. Proper data mining and data analysis can lead
to a proper description of the fraud, how it took place, what
controls were thwarted, the approximate level of loss and
even who committed the fraud. So the IT auditor can play an
invaluable role in gathering data, mining it, analyzing it, and
providing the lead investigator with evidence and information.
Also, the IT auditor can be an invaluable resource to convert
the mass of data into something that a judge or members of
a jury can easily understand and assimilate into their thought
processes (e.g., charts, diagrams, other high-tech visual aids).

But, usually, the data alone are insufficient to make a case,
even if it is a corporate investigation. A court case will likely
require more than just the data. Therefore, the IT auditor
needs to work closely with the lead investigator and others on
the investigation team, as the team will likely need to conduct
interviews and perform other tasks to collect more evidence
and information.
CONCLUSION
The IT auditor has a key role in fraud detection, prevention and investigation in today’s business world. It is important for the IT auditor to understand the key aspects of antifraud as it relates to IT audit. This knowledge could help the IT auditor be prepared to recognize a piece of fraud evidence, develop a sense of red flags and understand how certain fraud schemes are perpetrated. These five issues are a start in developing the knowledge and skills to be effective at detecting and investigating frauds.

ENDNOTE
1 The ACFE’s Report to the Nation is a regular report on fraud in the US. In the 1996, 2002 and 2004 reports, experts estimated fraud losses at 6 percent; in 2006, it was estimated at 5 percent; and, in 2008, it was estimated at 7 percent.
2 Ibid.
3 Based on the author’s experiences and the first-hand accounts of fraudsters such as Sam Antar (Crazy Eddie’s fraud) and Bill Owens (HealthSouth fraud).